- Does the email reference any consequences should you not 'verify your information'?
- Most important, remember that legitimate businesses should never ask for personal or financial information via email.

How Can I Avoid Becoming a Victim?

- If it appears to be a phishing email, simply delete it. You can also forward it to the company it claims to be from and to spam@uce.gov.
- Do not click on any links listed in the email message and do not open any attachments contained in the email. Many phishing messages and sites not only attempt to get your personal information, they also attempt to install malicious code, like a Trojan horse, on to your computer.
- Do not enter personal information in a pop-up screen. Legitimate companies, agencies and organizations don't ask for personal information via pop-up screens.
- Install a phishing filter on your email application and also for your web browser. These filters will not keep out all phishing messages, but it will reduce the numbers of phishing attempts.

Anything else I should do?

- Review your credit card and bank statements or bills from the companies you do business with, looking for unauthorized charges or withdrawals.

For more information on phishing visit:

AntiPhishing Work Group: www.antiphishing.org/
i-Safe Phishing Video: http://ftc.isafe.org/phishing.html
OnGuard Online: www.onguardonline.gov/phishing.html
National Consumer League's Internet Fraud Watch: www.fraud.org/tips/internet/phishing.htm
US CERT: www.us-cert.gov/cas/tips/ST04-014.html

For more monthly tips visit:

www.msisac.org/awareness/news/

Brought to you by:

MS-ISAC

http://www.msisac.org